Worksheet 3 Internet security Answers

Task 1

You are responsible for the network security of a new company with one office. It is suggested that a firewall and proxy server are required for the new system.

Describe the role of a firewall in providing security.

A firewall uses static filtering rules to allow or reject packets into (and out of) a network based on the protocols they are operating on. Any malicious packets attempting to gain access to disallowed ports are rejected immediately before they can deliver their payload.

What function does a proxy server serve, and can it provide additional security?

A proxy make external requests for resources such as web pages on behalf of an internal computer. This can provide anonymity for the user 'hiding' behind the proxy server.

Proxies can also provide content filtering, monitor bandwidth use and provide user logs of which devide requests have come from, when, and what users were looking at.

Another feature of a proxy server is the ability to store copies of web pages locally. This speeds up access to a previously visited web site as the proxy server can simply provide its own copy, rather than having to make an external request for a new copy.

Task 2

All employees use their own devices in the office.

The company owner wants to make new employees aware of the best practices for preventing the intrusion of malicious software into the network.

Write an overview that can be used to educate these new employees. You should explicitly mention:

- Preventing viruses
- Preventing worms
- Minimising the chance of phishing

Key points:

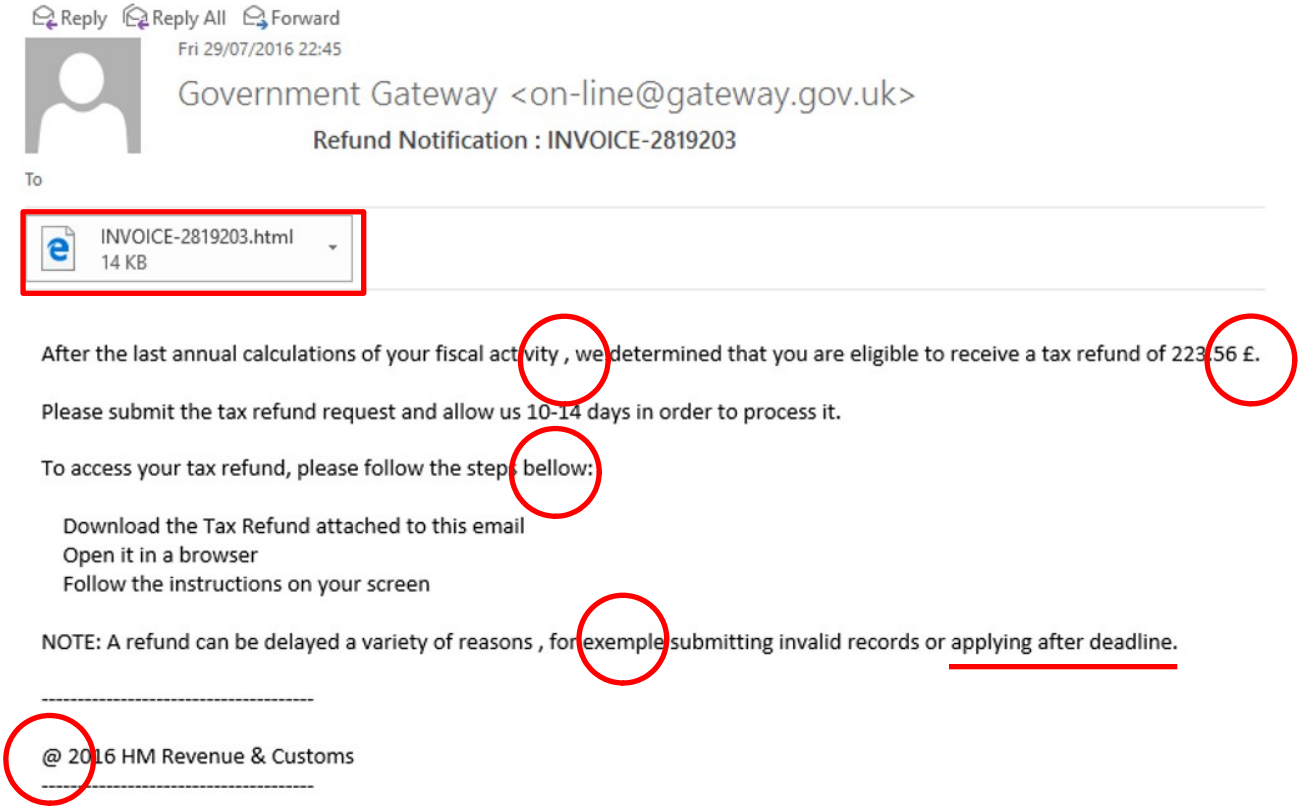
- Ensure anti-virus software is installed
- Make sure it is regularly updated
- Regularly update your operating system
- Do not open email attachments that you are not expecting
- Do not click on links in emails that seem suspicious
- Ensure passwords are difficult to guess

- Make sure you have a firewall installed
- Only enable the minimal amount of network access required to complete your work

Task 3

Social engineering is 'blagging' or tricking an individual into divulging their confidential details or information. The two email examples below may have come from confidence tricksters with malicious intent.

- What signs can you spot within these phishing emails that indicate they may not be from the advertised sender? Spelling, punctuation and gramattical errors; suspicious attachments; a sense of urgency expressed; suspect email addresses; poor formatting.



Reply Reply All Forward

Fri 29/07/2016 22:45

Government Gateway <on-line@gateway.gov.uk>

Refund Notification : INVOICE-2819203

To

INVOICE-2819203.html
14 KB

After the last annual calculations of your fiscal activity , we determined that you are eligible to receive a tax refund of 223.56 £.

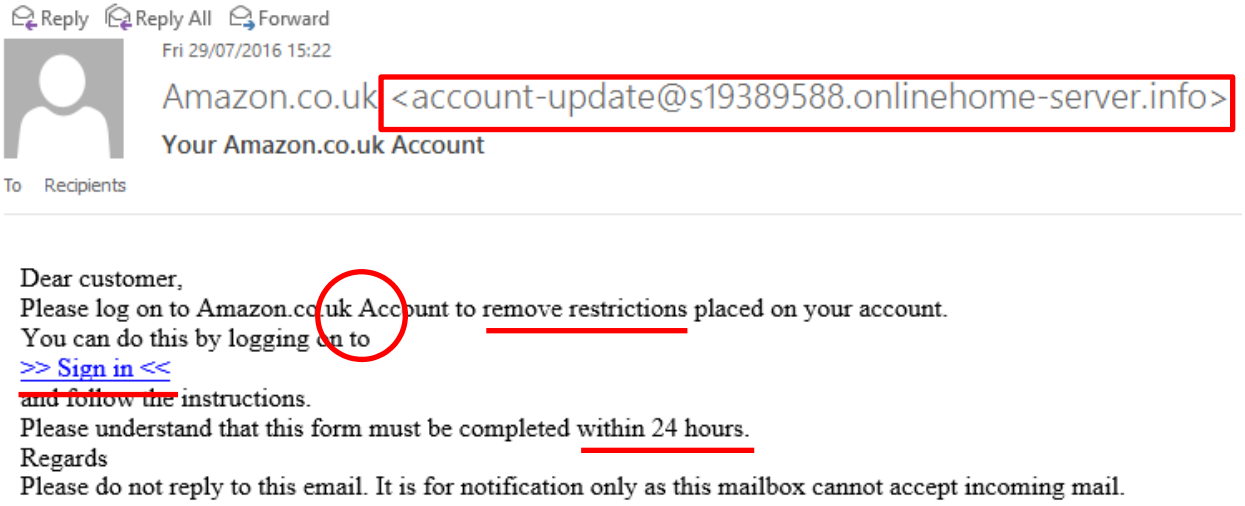
Please submit the tax refund request and allow us 10-14 days in order to process it.

To access your tax refund, please follow the steps bellow:

Download the Tax Refund attached to this email
Open it in a browser
Follow the instructions on your screen

NOTE: A refund can be delayed a variety of reasons , for exemple submitting invalid records or applying after deadline.

@ 2016 HM Revenue & Customs


Reply Reply All Forward
Fri 29/07/2016 15:22
Amazon.co.uk <account-update@s19389588.onlinehome-server.info>
Your Amazon.co.uk Account
To Recipients

Dear customer,
Please log on to Amazon.co.uk Account to remove restrictions placed on your account.
You can do this by logging on to
>> Sign in <<
and follow the instructions.
Please understand that this form must be completed within 24 hours.
Regards
Please do not reply to this email. It is for notification only as this mailbox cannot accept incoming mail.

- What might happen if you clicked on one of the links or opened the attachment? Trojans, or other malware may infect your computer. Your accounts details may be harvested and abused if you entered them in reponse.

Task 4

A University wants to set up and run a course on 'How to create a computer virus'. Discuss whether this is ethical?

Points against may include:

Should not be encouraging students / programmers to create malicious software.

Viruses created may be tested and run on the university network.

Is it generally wise?

Points for might include:

Training students to detect and delete viruses.

Increase awareness of the dangers of viruses.

Do software engineers who write commercial virus detection software programs need to understand how they are written in the first place? Should commercial virus software companies train people internally in virus creation?